UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,518	07/31/2001	Ernest E. Woodward	884.486US1	3616

21186 7590 06/16/2006

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
PYZOCHA, MICHAEL J	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/919,518	WOODWARD, ERNEST E.	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 April 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13 and 15-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13 and 15-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 and 15-27 are pending.

2. Amendment filed 04/20/2006 has been received and considered.

Claim Rejections - 35 USC § 103

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1-4, 6-9, and 15-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al (US 6385596), in view of Hardjono (US 6182214), in view of Johnston (US 6373946), in view of Arnold (US 6175924) and in view of Nakagawa (US 20020016775), further in view of Chang (US 6922735).

As per claim 1, Wiser et al discloses a method of controlling content usage in a communication device using a decryption key, the method comprises: providing the communication device a first key in response to a request for content; and verifying credit of a user of the personal communication device; providing the personal communication device a key when the credit is confirmed; for use in decrypting content (see column 4 lines 13-67).

Wiser et al fails to disclose the decryption key being broken into key-shares one of which is pre-stored on the device.

However Hardjono teaches the use of key-shares and pre-storing one on a device (see column 3 lines 33-42).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to distribute one of Hardjono's key-shares to each of the servers and users of Wiser et al to be delivered to the use upon request and confirmation of credit.

Motivation to do so would have been to set up a threshold cryptography system (see Hardjono column 3 lines 29-42).

The modified Wiser et al and Hardjono system fails to disclose the communications device is wireless.

However, Johnston teaches such wireless devices (see abstract).

At the time of the invention it would have been obvious to a person of ordinary skill in the art for the modified Wiser et al and Hardjono system's communications device to be wireless.

Motivation to do so would have been to communicate using satellite mobile telecommunications (see Johnston abstract).

The modified Wiser et al, Hardjono, and Johnston system fails to disclose the device having two processors and purging a key share when usage exceeds a measurement.

However, Arnold teaches a device with two processors and an authentication code (see figures 1 and 3); and Nakagawa teaches monitoring usage of content (see paragraphs 36-41).

At the time of the invention it would have been obvious to a person of ordinary skill in the art for the modified Wiser et al, Hardjono, and Johnston system to have two processors and monitor usage.

Motivation to do so would have been to protect secure memory (see Arnold column 2 lines 15-36) and to protect copyrights (see Nakagawa paragraph 11).

The modified Wiser et al, Hardjono, Johnston, Arnold and Nakagawa system fails to disclose the two or more processors are located on a single integrated circuit to prevent unauthorized interception of the content communicated between the processors.

However, Chang teaches the use of a single integrated circuit with two or more processors (see column 2 lines 44-62) and it is an inherent feature that when on a single integrated circuit the interception of communications is inhibited.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to include the multiple processor of the modified Wiser et al, Hardjono, Johnston, Arnold and Nakagawa system on a single integrated circuit.

Motivation to do so would have been to provide efficient communications (see Chang column 2 lines 3-10).

As per claim 7, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses a key-share pre-stored on a SIM combined to create a decryption key (see Johnston column 9 lines 14-21).

As per claim 8, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses the verifying credit of the user and the providing the second of the key-shares to the personal communication device are performed by a finance server in communication with the personal communication device (see Wiser et al column 4 lines 13-67 and figure 1).

As per claim 9, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses generating the key-shares from the decryption key using a key-splitting technique (see Hardjono column 3 lines 29-42).

As per claim 15, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses pre-storing the key-share before a request is sent (see Hardjono column 3 lines 29-42).

As per claim 4, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses receiving

the content from a content server in a security server; encrypting the content in the security server with the encryption key and providing the encrypted content from the security server to the personal communication device over a wireless communication link (see Wiser et al column 4 lines 13-67).

As per claim 6, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses the providing the first of the key-shares is performed by a security server in response to either the receipt of content at the security server or the encryption of the content by the security server in communication with the personal communication device (see Wiser et al column 4 lines 13-67).

As per claim 2, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses monitoring usage of the content with a security processor of the personal communications device; and purging a key-share when the usage exceeds a service limit indicated by the measurement parameters or when the authentication code fails to authenticate (see Nakagawa paragraphs 36-41).

As per claim 3, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses receiving the request for content from the wireless communication device,

the request identifying the content and the measurement parameters for the content encrypting the content where the key-share is pre-stored in the communications device (see Wiser et al column 4 lines 13-67 as applied above).

As per claim 10, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses the content comprises either video content or music content (see Wiser et al column 4 lines 13-67).

As per claims 11 and 19, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses generating a set of measuring parameters comprising at least one of a date-limit, a run-time limit, and an iteration limit, and wherein the personal communication device monitors usage of the content with respect to the measurement parameters and purges at least one of the key-shares when the usage exceeds one of the measurement parameters of the set (see Nakagawa paragraphs 36-41).

As per claim 12, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses a content server defining the set of measurement parameters based on preferences of a content provider (see Nakagawa paragraphs 36-41).

As per claim 13, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses the date-limit defines an end calendar date for playing the content, the nm-time limit defines a maximum amount of time for playing portions of the content, and the iteration limit defines a maximum number of times for playing the content or portions thereof (see Nakagawa paragraphs 36-41).

As per claims 16, 21, 24, 25 and 27, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses a security processor portion to combine a plurality of key-shares and decrypt content for the processing system, the security processor portion including a monitor for usage of the content constructed and arranged to purge at least one of the key-shares when the usage exceeds a measurement parameter; and a communications processor portion to receive decrypted content from the security processor portion and providing decrypted content for playing on the wireless communication device having a third key-share pre-stored and receiving the first and second key-shares (see Wiser et al as applied above).

As per claims 17 and 22, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses the security processor of the personal communication device purges at least one of the key-shares when usage of the content

exceeds a service limit indicated by the measurement parameters (see Nakagawa paragraphs 36-41).

As per claim 18, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses a key-share pre-stored on a SIM combined to create a decryption key (see Johnston column 9 lines 14-21).

As per claim 19, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses generating a set of measuring parameters comprising at least one of a date-limit, a run-time limit, and an iteration limit (see Nakagawa paragraphs 36-41).

As per claims 20 and 26, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses an applications processor portion to process applications running on the personal communication device, and wherein the security processor portion, communications processor portion and applications processor portion are part of a processor area and fabricated on an application specific integrated circuit (ASIC) (see Arnold figure 1).

As per claim 23, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system discloses the verifying credit of the user and the providing the second of the key-shares to the personal communication device are performed by

a finance server in communication with the personal communication device (see Wiser et al column 4 lines 13-67).

5. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system as applied to claim 4 above, and further in view of Howard et al (US 20020069365).

As per claim 5, the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system fails to disclose the security server and content server being separate entities.

However, Howard et al teaches a security and content server being separate (see paragraph 68).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to have the security and content servers of the modified Wiser et al, Hardjono, Johnston, Arnold, Nakagawa, and Chang system to be separate as in Howard et al.

Motivation to do so would be to allow them to be owned by separate people (see Howard et al paragraph 68).

Response to Arguments

6. Applicant's arguments with respect to claims 1-13 and 15-27 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Schell et al (US 5933503) teaches pre-storing a key in a processor area.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael

Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER